(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. März 2004 (25.03.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/025437 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00, H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP2003/009040

(22) Internationales Anmeldedatum:
14. August 2003 (14.08.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 39 062.2 26. August 2002 (26.08.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: SCHMIDT, Andreas [DE/DE]; Neustadtring 48, 38114 Braunschweig (DE). TRAUBERG, Markus [DE/DE]; Valkeakoskistr. 6, 38159 Velchede (DE).

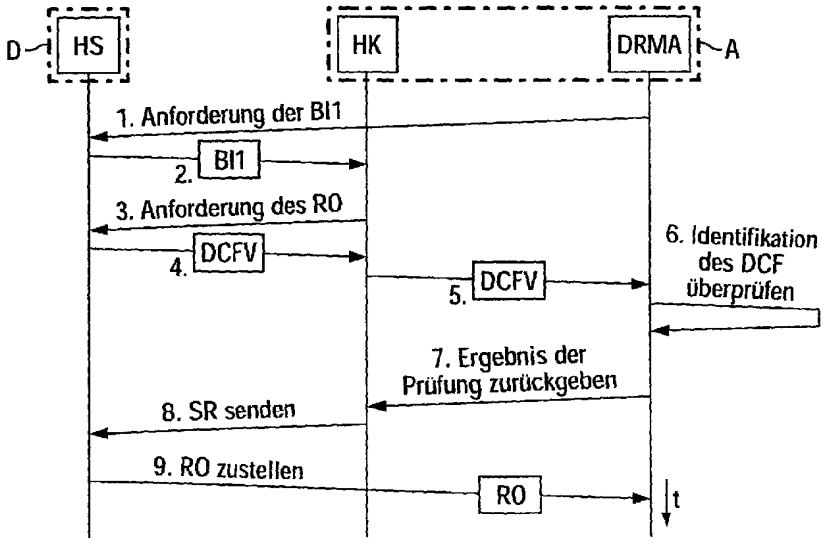
(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR TRANSMITTING ENCRYPTED USER DATA OBJECTS

(54) Bezeichnung: VERFAHREN ZUM ÜBERTRAGEN VON VERSCHLÜSSELTEN NUTZDATEN-OBJEKTEN



1 REQUEST BI1
3 REQUEST RO
6 VERIFY IDENTIFICATION OF DCF
7 RETURN RESULT OF VERIFICATION
8 TRANSMIT SR
9 SUPPLY RO

(57) Abstract: The invention relates to a method for handling, in particular transmitting encrypted user data objects. According to said method, a data preparation component (D) of a data preparation system provides user data objects. The data preparation component first encrypts a user data object that has been prepared. It then determines a checksum of the encrypted user data object and creates a container data object (DCF), in which the encrypted user data object and the determined checksum are provided. The container data object is subsequently transmitted to a first telecommunications device (A). Preferably, in order to use the encrypted user data object, the data preparation component (D) transmits descriptive information (BI1) containing a description of the possible usage rights for the encrypted user data object to the telecommunications device (A). After the selection of a specific rights object (RO), the data preparation device first transmits a confirmation object (DCFV) to the telecommunications device in order to verify the compatibility of the desired rights object and the encrypted user data object provided in the telecommunications device and if said verification is successful, subsequently transmits the rights object (RO) to the telecommunications device (A).

[Fortsetzung auf der nächsten Seite]

WO 2004/025437 A2

RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Offenbart ist ein Verfahren zum Handhaben, insbesondere Übertragen von verschlüsselten Nutzdaten-Objekten, bei dem eine Datenbereitstellungskomponente (D) eines Datenbereitstellungssystems Nutzdaten-Objekte bereitstellt. Dabei verschlüsselt die Datenbereitstellungskomponente zunächst ein auf ihr bereitgestelltes Nutzdaten-Objekt. Sie ermittelt ferner eine Prüfsumme des verschlüsselten Nutzdaten-Objekts und erzeugt ein Container-Datenobjekt (DCF), in dem das verschlüsselte Nutzdaten-Objekt sowie die ermittelte Prüfsumme vorgesehen wird. Anschließend wird das Container-Datenobjekt zu einer ersten Telekommunikationseinrichtung (A) übertragen. Vorteilhafterweise wird zur Nutzung des verschlüsselten Nutzdaten-Objekts von der Datenbereitstellungskomponente (D) eine Beschreibungsinformation (BI1) an die Telekommunikationseinrichtung (A) mit einer Beschreibung der möglichen Nutzungsrechte für das verschlüsselte Nutzdaten-Objekt gesendet. Nach Auswahl eines bestimmten Rechts bzw. Rechte-Objekts (RO) sendet die Datenbereitstellungskomponente zunächst ein Bestätigungsobjekt (DCFV) an die Telekommunikationseinrichtung zur Überprüfung der Kompatibilität des gewünschten Rechte-Objekts und des auf der Telekommunikationseinrichtung vorgesehenen, verschlüsselten Nutzdaten-Objekts und sendet dann bei erfolgreicher Überprüfung das Rechte-Objekt (RO) an die Telekommunikationseinrichtung (A).

Beschreibung

Verfahren zum Übertragen von verschlüsselten Nutzdaten-Objekten

Die vorliegende Erfindung betrifft ein Verfahren zum Handhaben, insbesondere Übertragen von verschlüsselten Nutzdaten-Objekten, die von einer Datenbereitstellungskomponente bereitgestellt und zu einer Telekommunikationseinrichtung wie beispielsweise einem Mobiltelefon, übertragen werden. Insbesondere betrifft die vorliegende Erfindung ein Verfahren, durch das ein Benutzer der Telekommunikationseinrichtung in die Lage versetzt wird, sich verschiedene Rechte bzw. Rechte-Objekte von der Datenbereitstellungskomponente auf die Telekommunikationseinrichtung gegen entsprechende Vergebührung herunterladen zu können.

Es wird derzeit ein Verfahren bzw. ein Dienst zum zuverlässigen und abrechenbaren Herunterladen von Nutzdaten-Objekten auf eine Telekommunikationseinrichtung, insbesondere in der Ausführung eines Mobilfunkgeräts oder Mobiltelefons, in einem Datenkommunikationsnetz diskutiert. Dabei soll das Herunterladen der Nutzdaten-Objekte zu dem Mobilfunkgerät mittels eines vom WAP-Forum (WAP: Wireless Application Protocol) spezifizierten Protokolls oder einem Internet-Protokoll (z.B. Hypertext Transfer Protocol: HTTP) erfolgen. Der Dienst zum Herunterladen ist dabei derart spezifiziert, dass einem Benutzer mit einem auf dem Mobilfunkgerät verfügbaren Anwendungsprogramm, das als ein Herunterlad-Klient bezeichnet wird, das Herunterladen von beliebigen Nutzdaten-Objekten ermöglicht werden soll, die von einem oder mehreren Datenbereitstellungskomponenten, insbesondere Servern bzw. Herunterlad-Servern von Dienstanbietern oder Inhaltanbietern, im Datenkommunikationsnetz angeboten werden. Eine mögliche Ausführung des Dienstes sieht vor, ein herunterladbares Nutzdaten-Objekt mit Restriktionen bzw. Beschränkungen bezüglich der Nutzung durch den Benutzer des Mobilfunkgeräts zu versehen. Beispielsweise kann damit die An-

zahl der Benutzungen des Nutzdaten-Objekts oder auch die Benutzungsdauer eingeschränkt werden. Die praktische Umsetzung erfolgt durch die Beschreibung der Restriktionen mit einer entsprechenden Sprache, wie beispielsweise der ODRL (Open Digital Right Expression Language), wobei der Herunterlad-Klient oder eine andere spezielle Anwendung, ein sogenannter DRM-Agent, zur Verwaltung der mit einem (digitalen) Nutzdaten-Objekt verknüpften Rechte (DRM: Digital Rights Management) die Rechtebeschreibung empfängt, auswertet, in einem geschützten, dem Benutzer nicht zugänglichen Speicherbereich auf dem Mobilfunkgerät ablegt und die Rechte bei einer Anfrage des Benutzers, das Objekt zu nutzen, entsprechend der Rechtebeschreibung gewährt oder nicht. Das Nutzdaten-Objekt selbst kann vor unauthorisiertem Zugriff entweder dadurch geschützt werden, dass es verschlüsselt in einem frei zugänglichen Speicherbereich auf dem Mobilfunkgerät abgelegt wird, oder dass es von einer speziellen Anwendung, beispielsweise dem DRM-Agenten, verwaltet wird, die keinen unautorisierten Zugriff auf das Objekt durch den Benutzer zulässt.

Gemäß einer vom WAP-Forum spezifizierten Variante für die Verwaltung von DRM-geschützten Inhalten wird ein von einer Datenbereitstellungskomponente bereitgestelltes Nutzdaten-Objekt verschlüsselt und wird schließlich zum Transport und zur Speicherung auf eine Telekommunikationseinrichtung, wie einem Mobilfunkgerät, in einer sogenannten Container-Datei bzw. einem sogenannten Container-Objekt verpackt (der beispielsweise den Datentyp oder Content-Typ "Application/VND.OMA.DRM.Content" zugewiesen bekommen hat). Mit einem Dienst zum zuverlässigen Herunterladen von Inhalten von einer Datenbereitstellungskomponente (Content Download) wird das verschlüsselte Nutzdaten-Objekt in dem Container-Objekt verpackt mittels WAP-Protokollen (wie beispielsweise dem WSP: Wireless Session Protocol) oder Internet-Protokollen (wie beispielsweise dem HTTP) auf die Telekommunikationseinrichtung übertragen. Separat vom verschlüsselten Nutzdaten-Objekt wird ein sogenanntes Rechte-Objekt auf die Telekommunikationseinrichtung, beispielsweise

mittels WAP-Push, übertragen. Das Rechte-Objekt enthält eine Beschreibung der Rechte, die dem Benutzer zur Nutzung des verschlüsselten Nutzdaten-Objekts gewährt werden, eine Referenz auf das Container-Objekt, die eine Zuordnung des Rechte-Objekts zum entsprechenden Container-Objekt ermöglicht, und einen Schlüssel, mit dem das verschlüsselte Nutzdaten-Objekt entschlüsselt werden kann, um es anschließend zu nutzen. Auf der Telekommunikationseinrichtung, wie dem Mobilfunkgerät, ist zur Nutzung der Kombination aus dem in dem Container-Objekt gepackten, verschlüsselten Nutzdaten-Objekt und dem Rechte-Objekt eine spezielle Einrichtung bzw. Anwendung notwendig, die der oben erwähnte DRM-Agent sein kann. Nach dem Übertragen des Rechte-Objekts auf die Telekommunikationseinrichtung wird das Rechte-Objekt direkt dem DRM-Agenten übergeben, der für die Verwaltung und Wahrung des Geheimnisses, nämlich des Schlüssels zum Entschlüsseln des verschlüsselten Nutzdaten-Objekts, verantwortlich ist. Praktisch legt der DRM-Agent das Rechte-Objekt vor einem unauthorisierten Zugriff durch andere Anwendungen oder Benutzer auf der Telekommunikationseinrichtung geschützt ab. Wenn ein verschlüsseltes Nutzdaten-Objekt genutzt werden soll, so wird zunächst der DRM-Agent aktiviert. Dieser sucht ein zu dem Container-Objekt passendes Rechte-Objekt in dem von ihm verwalteten Speicherbereich in der Telekommunikationseinrichtung anhand der im Container-Objekt und auch im Rechte-Objekt enthaltenen Identifikation, überprüft, ob für die angefragte Nutzungsart (wie beispielsweise ein "Abspielen" von Musikdaten oder ein "Anzeigen" von Bilddaten, usw.) Rechte gewährt werden können und entschlüsselt das Nutzdatenobjekt mit dem Schlüssel aus dem Rechte-Objekt, falls die Rechte gewährt werden können. Mit dem oben beschriebenen Verfahren, bei dem ein verschlüsseltes Nutzdatenobjekt und ein von diesem separates Rechte-Objekt verwendet werden können, wird der Wert digitaler Daten nicht mehr durch das (verschlüsselte) Nutzdaten-Objekt oder das Container-Objekt selbst, sondern vielmehr durch das Rechte-Objekt und dem darin enthaltenen Schlüssel dargestellt, ohne den ja das verschlüsselte Nutzdaten-Objekt nicht nutzbar ist. Somit können in diesem

Fall die verschlüsselten Nutzdaten-Objekte verpackt in den Container-Objekten frei zugänglich auf der Telekommunikationseinrichtung gespeichert werden. Auch das Weiterleiten verschlüsselter Nutzdaten-Objekte, verpackt in Container-Objekten, von einem Benutzer an einen oder mehrere Benutzer, als eine "Superdistribution" bezeichnet, wird damit möglich. Um das in einem weitergeleiteten Container-Objekt enthaltene, verschlüsselte Nutzdatenobjekt nutzbar zu machen, muss ein jeweiliger Benutzer von einem Rechteanbieter, der mit dem ein bestimmtes Nutzdaten-Objekt anbietenden Inhalteanbieter identisch sein kann, ein passendes Rechte-Objekt herunterladen.

Das gerade beschriebene Verfahren, bei dem zur Nutzbarmachung von Nutzdaten-Objekten zum einen ein Container-Objekt mit einem verschlüsselten Nutzdaten-Objekt, zum anderen ein Rechte-Objekt von einer identischen oder verschiedenen Datenbereitstellungskomponente(n) heruntergeladen werden müssen, hat jedoch den Nachteil, dass ein Benutzer vor dem Herunterladen eines Rechte-Objekts keine Möglichkeit hat, zu überprüfen, ob das angebotene Rechte-Objekt beispielsweise von einem beliebigen Anbieter tatsächlich die Nutzung des bereits auf der eigenen Telekommunikationseinrichtung vorhandenen, verschlüsselten Nutzdaten-Objekts in dem Container-Objekt ermöglicht, d.h. ob das angebotene Rechte-Objekt beispielsweise den passenden Schlüssel zur Entschlüsselung des in dem Container-Objekt enthaltenen, verschlüsselten Nutzdaten-Objekts umfasst. Ferner besteht der Nachteil, dass ein Benutzer ohne ein erworbenes bzw. heruntergeladenes Rechte-Objekt überhaupt keine Möglichkeit hat, zu überprüfen, ob das von seiner Telekommunikationseinrichtung empfangene, verschlüsselte Nutzdaten-Objekt oder auch das gesamte Container-Objekt unversehrt ist.

So ist es die Aufgabe der vorliegenden Erfindung, eine Möglichkeit zu schaffen, durch die ein Benutzer in die Lage versetzt wird, die Unversehrtheit bzw. Nutzbarkeit eines auf seiner Telekommunikationseinrichtung gespeicherten, verschlüsselten Nutzdaten-Objekts zu überprüfen.

Diese Aufgabe wird durch den Gegenstand der unabhängigen Ansprüche gelöst. Vorteilhafte Ausgestaltungen sind Gegenstand der Unteransprüche.

Dabei wird bei einem Verfahren zum Handhaben bzw. Übertragen von verschlüsselten Nutzdaten-Objekten, bei dem eine Datenbereitstellungskomponente Nutzdaten-Objekte bereitstellt, zunächst ein derartiges Nutzdaten-Objekt verschlüsselt, um es vor einem unberechtigten Zugriff zu sichern. Anschließend wird eine Prüfsumme des verschlüsselten Nutzdaten-Objekts (oder des gesamten Container-Objekts) ermittelt. Dies kann beispielsweise mittels eines herkömmlichen Hash-Algorithmus erfolgen. Es wird ferner eine Container-Datei bzw. ein Container-Objekt erzeugt, das einen Inhaltsabschnitt und einen Beschreibungsabschnitt aufweist. In dem Inhaltsabschnitt des Container-Objekts wird das verschlüsselte Nutzdaten-Objekt vorgesehen, während in dem Beschreibungsabschnitt die eben ermittelte Prüfsumme vorgesehen wird.Somit enthält das Container-Objekt zwei unabhängig voneinander untergebrachte Datenbereiche, die jedoch bezüglich ihres Inhalts (verschlüsseltes Nutzdatenobjekt zu von diesem ermittelten Prüfsumme) zusammenhängen und somit bei einem Vergleich dieser Daten eine Unversehrtheitsprüfung erlauben. Schließlich wird das erzeugte Container-Objekt zu einer ersten Telekommunikationseinrichtung eines ersten Benutzers übertragen.

Dabei sei bemerkt, dass es möglich ist, dass die noch unverschlüsselten Nutzdaten-Objekte von einer ersten Datenbereitstellungskomponente bereitgestellt werden, während sie von einer mit der ersten Datenbereitstellungskomponente verbundenen zweiten Datenbereitstellungskomponente verschlüsselt und zusammen mit einer diesbezüglich ermittelten Prüfsumme in ein Container-Objekt verpackt und schließlich einem Benutzer zum Herunterladen auf seine Telekommunikationseinrichtung angeboten werden. In einem derartigen Fall kann anstelle von einer oder mehreren einzelnen Datenbereitstellungskomponenten auch von einem Datenbereitstellungssystem gesprochen werden, das

die einzelnen Datenbereitstellungskomponenten zum Bereitstellen von Nutzdaten-Objekten bzw. zum Verschlüsseln, Packen und Anbieten von Nutzdaten-Objekten umfasst. Neben der Möglichkeit, dass ein Container-Objekt direkt von einer Datenbereitstellungskomponente bzw. einem Datenbereitstellungssystem zu einer einem Benutzer zugeordneten Telekommunikationseinrichtung übertragen wird, ist es auch möglich, dass das Container-Objekt über eine oder mehrere zweite bzw. weitere Telekommunikationseinrichtungen anderer Benutzer zum ersten Benutzer bzw. zu dessen Telekommunikationseinrichtung gelangt.

Vorteilhafterweise wird ein beispielsweise nach obigem Verfahren in einer Datenbereitstellungskomponente erzeugtes Container-Objekt nach dessen Erhalt von der ersten Telekommunikationseinrichtung derart analysiert, dass zunächst aus dem Beschreibungsabschnitt des Container-Objekts die dort vorgesehene Prüfsumme extrahiert wird. Anschließend wird von dem in dem Inhaltsabschnitt des Container-Objekts vorgesehenen verschlüsselten Nutzdaten-Objekt erneut die Prüfsumme ermittelt. Nun wird die gerade erneut ermittelte Prüfsumme mit der extrahierten Prüfsumme verglichen, um bei einer Übereinstimmung der beiden Prüfsummen auf eine ordnungsgemäße Übertragung des verschlüsselten Nutzdaten-Objekts bzw. auf eine Unversehrtheit des Nutzdaten-Objekt schließen zu können. Eine derartige Analyse eines erhaltenen Container-Objekts kann von einer speziellen Anwendung der (ersten) Telekommunikationseinrichtung durchgeführt werden, die speziell für die Verwaltung von Nutzungsrechten für digitale Daten oder Datenobjekte ausgelegt ist, nämlich einem sogenannten DRM-Agenten (DRM: Digital Rights Management). Ein derartiger Vergleich der extrahierten und neu ermittelten Prüfsumme ermöglicht somit festzustellen, ob insbesondere bei einer Superdistribution von Container-Objekten eine verschlüsseltes Nutzdaten-Objekt unvollständig übermittelt wurde oder ob ein Nutzdaten-Objekt beispielsweise gezielt manipuliert worden ist.

Es sei bemerkt, dass es möglich ist, dass in einem Container-Objekt bzw. in dessen Inhaltsabschnitt nicht nur ein verschlüsseltes Nutzdaten-Objekt vorgesehen sein kann, sondern auch eine Mehrzahl davon. Entsprechend muss von dieser Mehrzahl von verschlüsselten Nutzdaten-Objekten jeweils eine Prüfsumme ermittelt werden, wobei die jeweiligen Prüfsummen in dem Beschreibungsabschnitt des Container-Objekts vorzusehen sind. Bei einer Unversehrtheitsprüfung schließlich kann dann von jedem zu untersuchenden, verschlüsselten Nutzdaten-Objekt die jeweilige Prüfsumme ermittelt werden und mit der jeweiligen in dem Beschreibungsabschnitt vorgesehenen Prüfsumme verglichen werden. Somit ist es möglich, beispielsweise eine Vielzahl von zusammengehörigen Nutzdaten-Objekten (beispielsweise aufgrund ihrer thematischen Zusammengehörigkeit, wie Bilder eines gleichen Objekts in verschiedenen Auflösungen) in einem Container-Objekt zusammenzufassen und zu übertragen.

Um ein auf einer Telekommunikationseinrichtung vorgesehenes bzw. empfangenes, in einem Container-Objekt verpacktes, verschlüsseltes Nutzdaten-Objekt nutzen zu können, ist es notwendig, dass ferner ein Rechte-Objekt bereitgestellt wird, das zum einen eine Zuordnungsinformation zum Zuordnen des Rechte-Objekts zu einem verschlüsselten Nutzdaten-Objekt bzw. zu einem Container-Objekt, der das verschlüsselte Nutzdaten-Objekt enthält, aufweist. Ferner muss das Rechte-Objekt eine Entschlüsselungsinformation zum Entschlüsseln des verschlüsselten Nutzdaten-Objekts enthalten, um das Nutzdaten-Objekt für den Benutzer nutzbar zu machen, d.h. beispielsweise das Abspielen einer Musikdatei erlauben. Ferner kann das Rechte-Objekt eine Rechteinformation zur Beschreibung der Benutzungsrechte des verschlüsselten Nutzdaten-Objekts aufweisen. Die Benutzungsrechte können dabei beispielsweise beinhalten, wie lange die Nutzung eines Nutzdatenobjekts erlaubt wird, wie oft die Nutzung erlaubt wird, bzw. beispielsweise bei einem multimedialen Nutzdaten-Objekt die Nutzung welchen Mediums bei der Nutzung erlaubt ist (beispielsweise bei einem mit Musik unterlegten Videoclip, ob nur die Musik gehört werden darf oder auch der

zugehörige Videoclip angesehen werden darf). Das Rechte-Objekt kann beispielsweise von einer Datenbereitstellungskomponente erzeugt werden, die auch das Container-Objekt bereitstellt oder erzeugt, es kann jedoch auch von einer anderen Datenbereitstellungskomponente erzeugt werden, die beispielsweise wieder Teil eines übergeordneten Datenbereitstellungssystems ist.

Da wie bereits erwähnt, der Wert eines verschlüsselten Nutzdaten-Objekts vom zugeordneten Rechte-Objekt abhängt, das dem Benutzer die Nutzungsrechte für das Nutzdaten-Objekt einräumt, wird ein Anbieter von Rechte-Objekten (der auch mit dem Anbieter von Nutzdaten-Objekten identisch sein kann) nach Übersenden von einem Rechte-Objekt an einen Benutzer bzw. dessen Telekommunikationseinrichtung dem Benutzer das Rechte-Objekt unmittelbar in Rechnung stellen. Das bedeutet, der Benutzer, der beispielsweise aus einer Vielzahl von Rechte-Objekten auswählen kann, hätte somit keine Möglichkeit zu überprüfen, ob das ausgewählte Rechte-Objekt zu dem auf seiner Telekommunikationseinrichtung gespeicherten, verschlüsselten Nutzdaten-Objekt passt, bevor er das Rechte-Objekt herunterlädt und es bezahlen muss. Um somit einem Benutzer vor dem Übertragen bzw. Herunterladen eines bestimmten Rechteobjekts zu ermöglichen, zu überprüfen, ob das Rechteobjekt tatsächlich die Nutzung des bereits auf seiner Telekommunikationseinrichtung vorhandenen, verschlüsselten Nutzdaten-Objekts im Container-Objekt erlaubt, d.h. ob das bestimmte Rechte-Objekt den passenden Schlüssel zur Entschlüsselung des verschlüsselten Nutzdaten-Objekts enthalten wird, wird gemäß einer vorteilhaften Ausgestaltung ein dem Rechte-Objekt zugeordnetes Überprüfungsobjekt bzw. Bestätigungsobjekt erzeugt, das eine Zuordnungsinformation zum Zuordnen des Rechte-Objekts zu einem verschlüsselten Nutzdaten-Objekt und eine Prüfsumme des verschlüsselten Nutzdaten-Objekts aufweist. Das bedeutet, es wird in dem Datenbereitstellungssystem, insbesondere von der Datenbereitstellungskomponente, welche auch das Rechte-Objekt bereitstellt, ein Bestätigungsobjekt erzeugt, welches keine Entschlüsselung eines

verschlüsselten Nutzdaten-Objekts ermöglicht, jedoch eine Kompatibilitätsprüfung, ob ein dem Bestätigungsobjekt zugeordnetes Rechte-Objekt mit einem auf der Telekommunikationseinrichtung des Benutzers vorhandenen Nutzdaten-Objekt übereinstimmt bzw. kompatibel ist.

Diesbezüglich wird gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung seitens der ersten Telekommunikationseinrichtung an das Datenbereitstellungssystem eines Inhalteanbieters bzw. eine Datenbereitstellungskomponente von diesem eine Anforderung gestellt, dass das einem bestimmten Rechte-Objekt zugeordnete Bestätigungsobjekt an die (erste) Telekommunikationseinrichtung übertragen wird. Anschließend wird das Bestätigungsobjekt von der Datenbereitstellungskomponente bzw. dem Datenbereitstellungssystem zu der ersten Telekommunikationseinrichtung übertragen, wo schließlich die Prüfsumme aus dem Bestätigungsobjekt extrahiert wird. Es kann nun ein Vergleich zwischen der aus dem Bestätigungsobjekt extrahierten Prüfsumme und der erneut ermittelten Prüfsumme bzw. der in der Beschreibungsinformation des Container-Objekts vorgesehenen Prüfsumme durchgeführt werden, um bei einer Übereinstimmung der Prüfsummen auf eine Kompatibilität des dem Bestätigungsobjekt zugeordneten Rechte-Objekts und dem auf die erste Telekommunikationseinrichtung in dem Container-Objekt übertragenen, verschlüsselten Nutzdaten-Objekt schließen zu können. Das bedeutet, es ist nun möglich, ohne das eigentliche Rechte-Objekt übertragen zu müssen, mittels des dem Rechte-Objekt zugeordneten Bestätigungsobjekts bzw. der in diesem vorgesehenen Prüfsumme zu überprüfen, ob das Rechte-Objekt mit dem aus der Telekommunikationseinrichtung vorgesehenen Nutzdaten-Objekt kompatibel ist. Dabei ist es möglich, dass die Unversehrtheitsprüfung des im Container-Objekt enthaltenen, verschlüsselten Nutzdaten-Objekts vor dem Anfordern des Bestätigungsobjekts, während der Anforderung oder nach der Anforderung des Bestätigungsobjekts durchgeführt werden kann. Vorteilhafterweise wird die Unversehrtheitsprüfung jedoch nach Erhalt eines Container-Objekts und vor Anforderung eines Bestätigungsobjekt

oder Rechte-Objekts durchgeführt, um bei einem fehlerhaften, verschlüsselten Nutzdaten-Objekt bzw. Container-Objekt die Anforderung von Bestätigungs- oder Rechte-Objekten nicht unnötigerweise durchführen zu müssen.

Verläuft die Überprüfung des Bestätigungsobjekts bezüglich des in dem Container-Objekt vorhandenen, verschlüsselten Nutzdaten-Objekts positiv, so kann die (erste) Telekommunikationseinrichtung das positive Prüfungsergebnis in Form eines Statusberichts an die das Bestätigungsobjekt bzw. das diesem zugeordnete Rechte-Objekt bereitstellende Datenbereitstellungskomponente senden. Daraufhin kann diese von selbst das zugehörige Rechte-Objekt an die erste Telekommunikationseinrichtung übertragen. Es ist jedoch auch möglich, dass die erste Telekommunikationseinrichtung jedoch nicht sofort einen Statusbericht über die erfolgreiche Prüfung des Bestätigungsobjekts absendet, sondern zu einem späteren, von ihr bestimmten Zeitpunkt eine Anforderungsmitteilung an die das dem Bestätigungsobjekt zugeordnete Rechte-Objekt bereitstellende Datenbereitstellungskomponente sendet, damit diese schließlich das Rechte-Objekt an die erste Telekommunikationseinrichtung überträgt. Es ist jedoch auch möglich, dass die erste Telekommunikationseinrichtung lediglich nach einer Unversehrtheitsprüfung eines erhaltenen Container-Objekts direkt ein bestimmtes Rechte-Objekt von einer dieses bereitstellenden Datenbereitstellungskomponente mittels einer dafür vorgesehenen Anforderungsmitteilung anfordert.

Gemäß einem weiteren Aspekt wird bei einem Verfahren zum Handhaben bzw. Nutzbarmachen von verschlüsselten Nutzdaten-Objekten ein verschlüsseltes Nutzdaten-Objekts in einer ersten Telekommunikationseinrichtung bereitgestellt, beispielsweise indem es von einer Datenbereitstellungskomponente oder einer weiteren Telekommunikationseinrichtung übertragen worden ist und eventuell gemäß einem obigen Verfahren auf Unversehrtheit überprüft worden ist. Anschließend fordert die Telekommunikationseinrichtung eine Beschreibungsinformation bezüglich des

Inhalts des verschlüsselten Nutzdaten-Objekts von einer Datenbereitstellungskomponente an. Die angeforderte Beschreibungsinformation wird dann von der Datenbereitstellungskomponente an die erste Telekommunikationseinrichtung übertragen. Nun erfolgt in der Telekommunikationseinrichtung ein Überprüfen, ob der Inhalt mit in der Beschreibungsinformation angegebenen Eigenschaften von der ersten Telekommunikationseinrichtung nutzbar ist. Bei erfolgreicher Überprüfung der in der Beschreibungsinformation angegebenen Eigenschaften wird ein Bestätigungsobjekt von der Datenbereitstellungskomponente angefordert, das einem dem verschlüsselten Nutzdaten-Objekt zugeordneten Rechte-Objekt (RO) zugewiesen ist, um eine Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts zu überprüfen. Durch die Anforderung der Beschreibungsinformation ist es nun möglich, dass die Telekommunikationseinrichtung zunächst überprüft, ob das gespeicherte Nutzdaten-Objekt überhaupt nutzbar ist (hat die Telekommunikationseinrichtung beispielsweise keine Möglichkeit der Audio- oder Musikausgabe, so wäre ein Nutzdaten-Objekt mit einem Musikinhalt auf der Telekommunikationseinrichtung nicht nutzbar).

Vorteilhafterweise wird das Rechte-Objekt von der Datenbereitstellungskomponente zu der ersten Telekommunikationseinrichtung bei erfolgreicher Überprüfung der Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts übertragen.

Das verschlüsselte Nutzdaten-Objekt kann in einem Inhaltsabschnitt eines Container-Objekts vorgesehen sein. Ferner kann das Container-Objekt einen Beschreibungsabschnitt aufweisen, in dem eine Prüfsumme des verschlüsselten Nutzdaten-Objekts vorgesehen ist. Außerdem kann in dem Beschreibungsabschnitt des Container-Objekts ferner die Adresse der Datenbereitstellungskomponente zum Anfordern der Beschreibungsinformation und/oder des Bestätigungsobjekts vorgesehen sein.

Vorteilhafterweise weist das Bestätigungsobjekt eine Prüfsumme des verschlüsselten Nutzdaten-Objekts auf, wobei die Überprüfung der Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts durch folgende Schritte erfolgt. Es wird die Prüfsumme aus dem Bestätigungsobjekt extrahiert. Anschließend wird die aus dem Bestätigungsobjekt extrahierte Prüfsumme mit der in dem Beschreibungsabschnitt des Container-Objekts vorgesehenen Prüfsumme verglichen, um bei einer Übereinstimmung der beiden Prüfsummen auf eine Kompatibilität des dem Bestätigungsobjekt zugeordneten Rechte-Objekts und des auf die erste Telekommunikationseinrichtung in dem Container-Objekt vorgesehenen, verschlüsselten Nutzdaten-Objekts schließen zu können.

Wie bereits erwähnt, ist es möglich, dass bei erfolgreicher Kompatibilitätsprüfung des dem Rechte-Objekt zugeordneten Bestätigungsobjekts und dem auf der ersten Telekommunikationseinrichtung in dem Container-Objekt übertragenen, verschlüsselten Nutzdaten-Objekt eine erste Bestätigungsmitteilung von der ersten Telekommunikationseinrichtung zu der das Rechte- oder Bestätigungsobjekt bereitstellenden Datenbereitstellungskomponente übermittelt werden kann. Ferner ist es möglich, dass, sofern insbesondere keine Überprüfung des Rechte-Objekts mittels eines Bestätigungsobjekts durchgeführt wird, eine zweite Bestätigungsmitteilung von der ersten Telekommunikationseinrichtung zu der Datenbereitstellungskomponente gesendet wird, wenn die erste Telekommunikationseinrichtung das Rechte-Objekt von der Datenbereitstellungskomponente empfangen hat. Gemäß einer weiteren vorteilhaften Ausgestaltung wird dann dem Benutzer der ersten Telekommunikationseinrichtung aufgrund des Erhalts der ersten und/oder der zweiten Bestätigungsmitteilung von der Datenbereitstellungskomponente das übertragene Rechte-Objekt in Rechnung gestellt bzw. diesem eine Vergebührungsinformation zugesandt, so dass dieser das erhaltene Rechte-Objekt bezahlen kann.

Gemäß einer vorteilhaften Ausgestaltung sind die erste und/oder die weiteren Telekommunikationseinrichtungen sowie das Datenbereitstellungssystem einschließlich der in diesen vorgesehenen Datenbereitstellungskomponenten (für Container-Objekte, Bestätigungsobjekte oder Rechte-Objekte) Teil eines Telekommunikationsnetzes. Dabei ist es möglich, dass die erste und die weiteren Telekommunikationseinrichtungen jeweils Teil eines Telekommunikationsnetzes sind, wobei die einzelnen Telekommunikationseinrichtungen nicht Teil desselben Telekommunikationsnetzes sein müssen. Entsprechend kann eine Datenbereitstellungskomponente des Datenbereitstellungssystems, welche insbesondere als ein Datenserver eines Dienstanbieters oder Inhaltsanbieters ausgebildet ist, in einem Telekommunikationsnetz vorgesehen sein, das mit dem oder den Telekommunikationsnetzen, welche der ersten und den weiteren Telekommunikationseinrichtungen zugeordnet sind, verbunden ist.

Um das Verfahren zum Übertragen von Nutzdaten-Objekten möglichst flexibel nutzen zu können, können die erste und/oder die weiteren Telekommunikationseinrichtungen vorzugsweise als eine mobile Telekommunikationseinrichtung ausgebildet sein und dabei insbesondere ein Funkmodul bzw. Mobilfunkmodul umfassen. Die Telekommunikationseinrichtung kann dabei beispielsweise als ein Mobiltelefon, ein Schnurlostelefon, als ein Smartphone (Kombination aus einem kleinen tragbaren Computer und einem Mobiltelefon), als ein PDA (PDA: Personal Digital Assistant = persönlicher digitaler Assistent) bzw. als ein Organizer ausgebildet sein. Weiterhin können die Telekommunikationseinrichtungen auch andere mobil erreichbare Geräte umfassen, wie einen Personal Computer (PC) oder einen Laptop, die mittels eines angeschlossenen Mobilfunkgeräts (Mobiltelefon) über ein Mobilfunknetz erreicht werden können. Das Mobilfunkgerät kann dann beispielsweise über ein Kabel an den Personal Computer bzw. Laptop angeschlossen sein oder auch diese drahtlos über eine Infrarot-Schnittstelle oder ein lokales Bluetooth-Netz kontaktieren. Dabei kann die erste und/oder auch die weiteren Telekommunikationseinrichtungen einschließlich des diesen zu-

geordneten Telekommunikationsnetzes in der Ausführung eines Mobilfunknetzes gemäß dem GSM (Global System for Mobile Communication)-Standard oder dem UMTS (Universal Mobile Telecommunications System)-Standard arbeiten. Derartige Mobilfunknetze bzw. Telekommunikationseinrichtungen gemäß dem GSM- oder UMTS-Standard können eine Plattform für WAP-Protokolle bzw. den WAP-Protokoll-Stack (WAP: Wireless Application Protocol) darstellen, mittels dem Daten (Mitteilungen bzw. Nutzdaten-Objekte) im jeweiligen Mobilfunknetz übertragbar sind. Im Falle der Verwendung des WAP-Protokoll-Stack ist es möglich, durch die Verwendung eines WAP-Gateways als Schnittstelle zwischen einem Mobilfunknetz und einem anderen Netzwerk, beispielsweise einem auf einem Internet-Protokoll basierenden Netz, eine Verbindung zu diesem zu schaffen. Auf diese Weise ist es möglich, dass sich die Datenbereitstellungskomponenten in einem auf einem Internet-Protokoll basierenden Netzwerk, wie dem Internet, befindet, wobei die Daten (Mitteilungen, Nutzdaten-Objekte) über ein WAP-Gateway und schließlich über eine Luftschnittstelle eines Mobilfunknetzes zwischen der oder den Basisstationen des Mobilfunknetzes und an die jeweiligen Telekommunikationseinrichtungen übertragen werden können.

Gemäß einer vorteilhaften Ausgestaltung kann es sich bei den Nutzdatenobjekten um Daten in Form von Textdaten, Bilddaten bzw. Videodaten, Audiodaten, ausführbare Programme oder Softwarekomponenten oder eine Kombination dieser Datenarten, d.h. um multimediale Daten bzw. Inhalte, handeln.

Bevorzugte Ausführungsformen der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

Figur 1 ein Blockschaltbild mit den bei einem Verfahren zum Herunterladen von Nutzdaten-Objekten beteiligten Komponenten einschließlich des Datenflusses zwischen den Komponenten;

Figur 2 ein Blockschaltbild mit den bei einem Verfahren zum Herunterladen bzw. Übertragen von Rechte-Objekten beteiligten Komponenten einschließlich des Datenflusses zwischen den Komponenten;

Figur 3 eine schematische Darstellung eines Container-Objekts gemäß einer Ausführungsform der Erfindung;

Figur 4 eine schematische Darstellung eines Rechte-Objekts gemäß einer Ausführungsform der Erfindung;

Figur 5 eine schematische Darstellung eines dem Rechte-Objekt zugeordneten Bestätigungsobjekts gemäß einer Ausführungsform der Erfindung.

Ein von dem WAP-Forum bzw. dessen Nachfolgeorganisation OMA (OMA: Open Mobile Alliance) vorgeschlagenen Verfahren zum Herunterladen bzw. Übertragen beliebiger Datenobjekte auf Telekommunikationseinrichtungen, wie Mobilfunkgeräte oder Mobiltelefone, und zur Verwaltung der Rechte für die (digitalen) Nutzdaten-Objekte besteht im wesentlichen aus zwei Abschnitten, nämlich dem eigentlichen Herunterladen bzw. Übertragen der Nutzdatenobjekte ("Content Download") und der Verwaltung der digitalen Rechte ("Digital Rights Management").

Wie es in Figur 1 zu sehen ist, umfasst eine Telekommunikationsanordnung zum Durchführen eines Verfahrens zum Herunterladen bzw. Übertragen von Nutzdaten-Objekten eine Datenbereitstellungskomponente zum Bereitstellen von Nutzdaten-Objekten sowie eine (erste) Telekommunikationseinrichtung A. Die Telekommunikationseinrichtung ist im Beispiel als ein Mobiltelefon ausgebildet, welches nach dem GSM- oder dem UMTS-Standard arbeiten kann. Es sei ferner angenommen, dass das Mobiltelefon A Teil eines Mobilfunknetzes ist. Das Mobiltelefon A ist in der Lage, WAP-Protokolle (z.B. Wireless Session Protocol: WSP, usw.) bzw. den WAP-Protokoll-Stack zu verwenden, um Daten über eine Luftschnittstelle an eine entsprechende stationäre Sende-

/Empfangsanordnung des dem Mobiltelefon A zugeordneten Mobilfunknetzes zu übertragen. Die Datenbereitstellungskomponente D kann in dem dem Mobiltelefon A zugeordneten Mobilfunknetz vorgesehen sein oder kann beispielsweise im Internet vorgesehen sein, das über entsprechende WAP-Gateways mit dem Mobilfunknetz des Mobiltelefons A verbunden ist. Obwohl es möglich ist, dass ein Nutzdaten-Objekt nicht nur direkt von der Datenbereitstellungskomponente D an das Mobiltelefon A übertragen werden kann, sondern auch über weitere Datenbereitstellungskomponenten, die zusammen ein Datenbereitstellungssystem bilden, oder aber auch über weitere Mobiltelefone übertragen werden können, sei für die folgende Erläuterung der Einfachheit halber die direkte Übertragung von Nutzdaten-Objekten von der Datenbereitstellungskomponente D zu dem Mobiltelefon A erläutert.

Wie es in den in Figur 1 bezeichneten Komponenten zu erkennen ist, werden für ein Verfahren zum Übertragen bzw. Herunterladen von Nutzdaten-Objekten zwei logische Einheiten benötigt, nämlich zum einen ein sogenannter "Herunterlad-Server" und ein sogenannter "Herunterlad-Klient":

1.) Der Herunterlad-Server HS, der insbesondere durch eine Softwareanwendung bzw. ein Softwareprogramm auf einer Datenbereitstellungskomponente, wie einem Datenserver, realisiert wird, hat zum einen die Aufgabe, den Herunterlad-Klienten auf einer Telekommunikationseinrichtung bzw. einem Mobiltelefon zunächst Beschreibungsinformationen über ein bestimmtes, von dem Herunterlad-Server verwaltetes Objekt bereitzustellen. Derartige Beschreibungsinformationen werden auch als Meta-Daten oder als Objekt-Beschreibung bezeichnet. Auf der Basis einer Anforderung durch einen Benutzer eines Herunterlad-Klienten auf dessen Telekommunikationseinrichtung stellt der Herunterlad-Server diesem ein gewünschtes Nutzdaten-Objekt zu. Dabei kann der Herunterlad-Server zuvor optional übermittelte Eigenschaften des Herunterlad-Klienten bzw. der Telekom-

munikationseinrichtung, auf der dieser ausgeführt wird, oder eines an die Telekommunikationseinrichtung angeschlossenen Geräts berücksichtigen, indem vom Herunterlad-Server ein an die Eigenschaften angepasstes Nutzdaten-Objekt ausgewählt oder speziell für den Herunterlad-Klienten, der als aktueller Empfänger dient, erzeugt wird.

2.) Der Herunterlad-Klient HK stellt insbesondere eine Softwareanwendung auf einer Telekommunikationseinrichtung, wie dem Mobiltelefon A, oder eine Anwendung auf einer mit der Telekommunikationseinrichtung verbundenen Datenverwaltungsvorrichtung, wie beispielsweise einem tragbaren Computer oder einem PDA, dar. Der Herunterlad-Klient handelt zunächst die Auslieferung eines gewünschten Nutzdaten-Objekts mit dem Herunterlad-Server aus, empfängt dieses und bestätigt dem Herunterlad-Server den fehlerfreien Empfang und eventuell auch die Nutzbarkeit des empfangenen Inhalts auf der Telekommunikationseinrichtung bzw. dem Mobiltelefon A, wie es im Beispiel verwendet wird.

Der Vorgang zum Herunterladen bzw. zur Übertragung von Nutzdaten-Objekten von dem Herunterlad-Server zu dem Herunterlad-Klienten, wie er unten noch bezüglich Figur 1 erläutert werden wird, ist derart ausgelegt, dass er folgende Anforderungen erfüllt:

Bevor ein Benutzer ein Nutzdaten-Objekt von einer Datenbereitstellungskomponente herunterlädt, muss er wie bereits erwähnt, zunächst über die Eigenschaften des Nutzdaten-Objekts informiert werden (beispielsweise durch eine Objektbeschreibung bzw. eine Beschreibungsinformation). Entsprechende Informationen können unter anderem sein: der Name des Nutzdaten-Objekts, das Datenvolumen zur Übertragung des Nutzdaten-Objekts (z.B. in Bytes), eine (verbale) Beschreibung des Nutzdaten-Objekts und beliebige weitere Eigenschaften des herunterzuladenden Nutzdaten-Objekts.

Der Nutzer muss seine explizite Zustimmung (Annahme des Angebots von der Datenbereitstellungskomponente) für die Auslieferung und eventuell die Abrechnung des Nutzdaten-Objekts erteilen können.

Es sei nochmals auf Figur 1 Bezug genommen, in der der Vorgang des Herunterladens eines Nutzdaten-Objekts ausführlich dargestellt ist, wobei der zeitliche Nachrichtenfluss und Aktionsablauf mit den Zahlen an den Pfeilen in Figur 1 gekennzeichnet ist:

1.) Der Herunterlad-Klient HK auf dem Mobiltelefon A fordert eine Beschreibungsinformation BI1 vom Herunterlad-Server der Datenbereitstellungskomponente D an, welche die Objektbeschreibung bzw. Meta-Daten über ein bestimmtes Nutzdaten-Objekt enthält.

2.) Die Beschreibungsinformation BI1 wird von dem Herunterlad-Klienten HK von dem Herunterlad-Server HS übertragen. Auf der Basis der erhaltenen Beschreibungsinformationen kann die Verwendbarkeit des beschriebenen Nutzdaten-Objekts auf dem Mobiltelefon A des Benutzers überprüft werden und weiterhin die Zustimmung des Benutzers zum Herunterladen des Nutzdaten-Objekts eingeholt werden (hier nicht explizit dargestellt).

3.) Der Herunterlad-Klient HK fordert das Nutzdaten-Objekt vom Herunterlad-Server HS an.

4.) Der Herunterlad-Server HS sendet das ausgewählte Nutzdaten-Objekt an den Herunterlad-Klienten HK.

5.) Der Herunterlad-Klient HK sendet seinerseits einen Statusbericht bzw. Statusreport SR an den Herunterlad-Server HS zurück.

Gemäß einer bereits eingangs beschriebenen Variante zur Verhinderung eines unbefugten Zugriffs auf ein Nutzdaten-Objekt bzw. einer unbefugten Verwendung eines heruntergeladenen Datenobjekts wird von einer Datenbereitstellungskomponente eines Datenbereitstellungssystems ein Nutzdaten-Objekt verschlüsselt und zusammen mit einer Prüfsumme des Nutzdaten-Objekts in einem Container-Objekt bzw. einer Container-Datei vorgesehen. Derartige Container-Objekte können dann gemäß dem gleichen Verfahren übertragen werden, wie es beispielsweise für unverschlüsselte Nutzdaten-Objekte in Figur 1 bereits dargestellt worden ist.

Ausgehend von einem derartigen Fall, bei dem ein in einem Container vorgesehenes, verschlüsseltes Nutzdaten-Objekt auf der Telekommunikationseinrichtung eines Benutzers vorliegt, ist es nun notwendig, dass der Benutzer der Telekommunikationseinrichtung sich die Rechte zur Nutzung des übertragenen Container-Objekts besorgt. Derartige Rechte können gemäß der im Folgenden beschriebenen Ausführungsform mittels eines Rechte-Objekts von der Datenbereitstellungskomponente zu der Telekommunikationseinrichtung des Benutzers übertragen werden. Ein derartiges Rechte-Objekt, das später noch bezüglich Figur 4 erläutert werden wird, enthält beispielsweise eine Beschreibung der Rechte, die den Benutzer zur Nutzung des in dem Container-Objekt vorgesehenen, verschlüsselten Nutzdaten-Objekts gewährt werden, eine Referenz auf das Container-Objekt, die eine Zuordnung des Rechte-Objekts zum entsprechenden Container-Objekt ermöglicht, und einen Schlüssel, mit dem das verschlüsselte Nutzdaten-Objekt entschlüsselt werden kann, um es anschließend zu nutzen. Wie es ferner bezüglich 2 noch erläutert werden wird, ist es notwendig, dass zur Nutzung der Kombination aus dem verschlüsselten Nutzdaten-Objekt ein Container-Objekt und ein Rechte-Objekt eine spezielle Einrichtung bzw. Softwareanwendung auf der Telekommunikationseinrichtung des Benutzers vorgesehen ist, die als ein sogenannter DRM (Digital Rights Management)-Agent bezeichnet wird. Der DRM-Agent erhält das Rechte-Objekt, das von einer Datenbereitstellungs-

komponente zur Telekommunikationseinrichtung übertragen worden ist, und ist für die Verwaltung des Rechte-Objekts bzw. die Verwahrung dessen Geheimnisses, d.h. den Schlüssel zum Entschlüsseln des verschlüsselten Nutzdaten-Objekts im Container-Objekt, verantwortlich. Praktisch muss der DRM-Agent das Rechte-Objekt vor einem unautorisierten Zugriff durch andere Einrichtungen bzw. Anwendungen auf der Telekommunikationseinrichtung geschützt ablegen. Bei einem in Figur 2 unten zu erläuternden Verfahren gemäß einer Ausführungsform der Erfindung, bei dem Rechte bzw. Rechte-Objekte unabhängig von (in Container-Objekten verpackten und verschlüsselten) Nutzdaten-Objekten an eine Telekommunikationseinrichtung eines Benutzers übertragen werden, sollen dabei die folgenden Kriterien berücksichtigt werden:

- Es soll eine Überprüfung der Integrität bzw. Unversehrtheit eines Container-Objekts bzw. des in diesem enthaltenen, verschlüsselten Nutzdaten-Objekts möglich sein, auch wenn das Container-Objekt per "Superdistribution" auf die Telekommunikationseinrichtung eines Benutzers übertragen wurde, und potentiell aus einer unzuverlässigen Quelle stammt. Zu diesem Zweck wird gemäß einer bevorzugten Ausführungsform der Erfindung von einer Datenbereitstellungskomponente eine Prüfsumme des verschlüsselten Nutzdaten-Objekts als zusätzliches Informationselement in einen Beschreibungsabschnitt des Container-Objekts eingefügt (vgl. dazu auch Figur 3). Die Prüfsumme kann dabei auch mit einer Hash-Funktion bzw. einem Hash-Algorithmus berechnet werden. Eine Hash-Funktion kann dabei aus einem Datenobjekt beliebiger Größe eine Zeichen-folge fester Länge (z.B. 128 oder 160 Bit) mit folgenden Eigenschaften berechnen. Die Zeichenfolge ist für das Datenobjekt eindeutig ("digitaler Fingerabdruck"). Selbst die Änderung eines einzigen Bits des Datenobjekts ergibt einen völlig anderen Hash-Wert. Das ursprüngliche Datenobjekt kann aus dem Hash-Wert nicht rekonstruiert werden. Es ist praktisch unmöglich, zwei Datenobjekte zu finden, die den gleichen Hash-Wert ergeben. Alternativ kann die Prüf-

summe bzw. der Hash-Wert auch über das gesamte Container-Objekt berechnet werden. Der oben erwähnte DRM-Agent zur Verwaltung von Rechten eines Nutzdaten-Objekts auf einer Telekommunikationseinrichtung eines Benutzers kann somit Integrität bzw. Unversehrtheit des verschlüsselten Nutzdaten-Objekts nur auf der Basis des Container-Objekts überprüfen, indem er mit dem definierten und allgemein bekannten Algorithmus zur Berechnung der Prüfsumme bzw. des Hash-Werts eben diese/diesen für das verschlüsselte Nutzdaten-Objekt oder das gesamte Container-Objekt berechnet und mit der/dem im Container-Objekt vergleicht.

- Der Benutzer soll in der Lage sein, neue Rechte bzw. Rechte-Objekte für ein auf seiner Telekommunikationseinrichtung vorgesehenes in einem Container-Objekt verpacktes, verschlüsseltes Nutzdaten-Objekt anzufordern. Zu diesem Zweck kann in dem Container-Objekt, genauer gesagt in dessen Beschreibungsabschnitt (vgl. Figur 3), eine Ressource ("rights-issuer") angegeben sein, von der der DRM-Agent ein Herunterladen eines Rechte-Objekts, entsprechend dem in Figur 1 dargestellten Herunterladen von Nutzdaten-Objekten, startet. Dies ermöglicht das Herunterladen von Rechten bzw. Rechte-Objekten auf die Telekommunikationseinrichtung mit der Zuverlässigkeit entsprechend dem "normalen" Herunterladvorgang für Nutzdaten-Objekte. Genauer gesagt kann in dem Beschreibungsabschnitt des Container-Objekts eine URL (URL: Uniform Resource Locator) vorgesehen sein, die beispielsweise eine "Adresse" für eine bestimmte Datenbereitstellungskomponente, die identisch mit der Datenbereitstellungskomponente für Nutzdaten-Objekte sein kann, angibt. Durch das Aufrufen der angegebenen URL durch eine der Anwendungen, Herunterlad-Klient oder DRM-Agent, kann einem Benutzer (beispielsweise über eine Menüstruktur) ein Angebot über ein oder mehrere verschiedene Rechte bereitgestellt werden, wobei er sich ein bestimmtes bzw. bestimmte Rechte in Form von Rechte-Objekten durch einen Herunterladevorgang zukommen lassen oder erwerben kann. Dem Benutzer

wird somit eine bekannte Schnittstelle und Bedienung angeboten, wie er sie bereits vom Herunterladen von Nutzdaten-Objekten auf seine Telekommunikationseinrichtung kennt, was das Vertrauen in den Dienst erhöht.

- Um zu gewährleisten, dass ein bestimmtes ausgewähltes Rechte-Objekt (das sich auf einer Datenbereitstellungskomponente befindet) zu einem auf der Telekommunikationseinrichtung eines Benutzers befindlichen Container-Objekt oder dem darin verpackten, verschlüsselten Nutzdaten-Objekt passt, und um somit zu verhindern, dass einem Benutzer einer Telekommunikationseinrichtung ein falsches Rechte-Objekt übermittelt wird, das er jedoch bezahlen muss, soll zunächst anstelle des Rechte-Objekts ein diesem zugeordnetes Bestätigungsobjekt ("verifier object") zur Telekommunikationseinrichtung des Benutzers übertragen werden. In diesem Bestätigungsobjekt ist die Prüfsumme bzw. der Hash-Wert des auf der Telekommunikationseinrichtung des Benutzers bereits vorhandenen, in einem Container-Objekt verpackten, verschlüsselten Objekts bzw. die Prüfsumme (der Hash-Wert) des Container-Objekts enthalten. Ferner kann das Bestätigungsobjekt eine Identifikationsbezeichnung für das zu überprüfende Container-Objekt enthalten, damit der für die Rechteverwaltung zuständige DRM-Agent in der Lage ist, das richtige auf der Telekommunikationseinrichtung des Benutzers gespeicherte Container-Objekt zu überprüfen. Das bedeutet, es wird ein neuer Objekttyp, nämlich der des Bestätigungsobjekts definiert, mit dem DRM-relevante Daten von dem Herunterlad-Server einer Datenbereitstellungskomponente zu dem DRM-Agenten einer Telekommunikationseinrichtung übertragen werden können, ohne dass das eigentliche Rechte-Objekt übertragen werden muss. Dadurch wird eine Trennung von DRM-relevanten Daten und inhaltsbezogenen Daten und eine Realisierung eines prinzipiell gleichen Ablaufs des Herunterladevorgangs für zusätzliche Rechte bzw. Rechte-Objekte bei zusätzlicher Gewährleistung der Zusammengehörigkeit von bereits auf der Telekommunikationseinrichtung

eines Benutzers vorhandenem, verschlüsselten Nutzdaten-Objekt und herunterzuladendem Rechte-Objekt geschaffen.

- Gemäß einer möglichen Ausgestaltung der erläuterten Ausführungsform überprüft der DRM-Agent bereits vor oder während der Anforderung neuer Rechte bzw. Rechte-Objekte die Prüfsumme oder den Hash-Wert bezüglich des Container-Objekts oder des darin verpackten, verschlüsselten Nutzdaten-Objekts auf Richtigkeit bzw. Unversehrtheit. Damit reduziert sich der Aufwand für die Überprüfung der Prüfsumme bzw. des Hash-Werts nach Erhalt des Bestätigungsobjekts auf einen Vergleich zwischen der gerade überprüften bzw. erneut ermittelten Prüfsumme (oder dem Hash-Wert) und der in dem Bestätigungsobjekt vorgesehenen Prüfsumme (oder dem Hash-Wert). Somit kann dann eine Zeit zum Versenden eines Statusberichts an den Herunterladserver nach erfolgtem Vergleich bzw. die Zeit zum Anfordern des eigentlichen Rechte-Objekts verringert werden.

- Ist die Überprüfung der von dem Bestätigungsobjekt übertragenen Prüfsumme (dem Hash-Wert) negativ, d.h. stimmt die in dem Bestätigungsobjekt vorgesehene Prüfsumme nicht mit der von dem DRM-Agenten erneut ermittelten Prüfsumme von dem verschlüsselten Nutzdaten-Objekt oder dem gesamten Container-Objekt nicht überein, so kann der Herunterladevorgang des eigentlichen Rechte-Objekts unterbrochen werden, wodurch der Benutzer der Telekommunikationseinrichtung, der ein Rechte-Objekt herunterladen wollte, davor geschützt wird, ein für ihn unbrauchbares Rechte-Objekt herunterzuladen und somit davor geschützt wird, dieses unbrauchbare Rechte-Objekt bezahlen zu müssen.

Im Folgenden soll nun ein Ablaufschema zur Darstellung des Verfahrens zum Übertragen bzw. Herunterladen von Rechten bzw. einem Rechte-Objekt anhand von Figur 2 dargestellt werden, wobei der zeitliche Datenfluss und Verfahrensablauf mit den Zahlen von 1. bis 9. an den Pfeilen von Figur 2 gekennzeichnet

ist. Es wird in diesem Fall davon ausgegangen, dass auf der Telekommunikationseinrichtung eines Benutzers, auf die ein Rechte-Objekt übertragen werden soll, bereits ein in einem Container-Objekt verpacktes und verschlüsseltes Nutzdaten-Objekt in einem Speicherbereich der Telekommunikationseinrichtung vorgesehen ist, das beispielsweise durch ein in Figur 1 dargestelltes Verfahren zum Herunterladen von Nutzdaten-Objekten von einer Datenbereitstellungskomponente stammt oder von einer anderen Telekommunikationseinrichtung übertragen worden ist. Ferner wird in Figur 2 davon ausgegangen, dass es sich bei dem Herunterladserver HS entsprechend Figur 1 um eine Anwendung auf einer Datenbereitstellungskomponente D eines Datenbereitstellungssystems handelt, während es sich bei dem Herunterlad-Klient HK und dem DRM-Agenten DRMA um Anwendungen bzw. Software-Anwendungen auf einer Telekommunikationseinrichtung bzw. einem Mobiltelefon A eines Benutzers handelt, auf das ein bestimmtes Rechte-Objekt übertragen werden soll.

1.) Zum Herunterladen bzw. zum Übertragen eines Rechte-Objekts RO wird von dem DRM-Agenten DRMA eine Ressource des Rechteanbieters (Datenbereitstellungskomponente D) mittels der entsprechenden URL, die in dem Beschreibungsabschnitt des entsprechenden Container-Objekts auf dem Mobiltelefon A des Benutzers angegeben ist, angefordert bzw. aufgerufen. Damit wird ein neuer Herunterladevorgang gestartet. Ziel der Anforderung ist der Erhalt einer Beschreibungsinformation, die zum Mobiltelefon A übertragen wird und dort entsprechend vom Herunterlade-Klienten HK ausgewertet und beantwortet wird. Alternativ kann auch eine Browsing-Sitzung zwischen dem Abrufen der Ressource durch den DRM-Agenten und der Übertragung der Beschreibungsinformation BI1 erfolgen, d.h. die unmittelbare Antwort auf die anfängliche Anforderung bzw. Anfrage im Agenten DRMA enthält nicht eine Beschreibungsinformation, sondern eine oder mehrere Web-Seiten, die beispielsweise ein Angebot zum Herunterladen neuer Rechte beschreiben und einen Verweis zum Herunterladen der Beschreibungsin-

formation enthalten. Am Ende der Browsing-Sitzung wird jedoch nach Auswahl eines bestimmten Rechte-Objekts wieder eine Beschreibungsinformation von dem Mobiltelefon A bzw. dem DRM-Agenten angefordert.

2.) Die Beschreibungsinformation BI1 wird an das Mobiltelefon A übertragen und anhand ihres Typs an den Herunterlad-Klienten HK übergeben. Dabei kann die Übertragung der Beschreibungsinformation von der Datenbereitstellungskomponente D an das Mobiltelefon A beispielsweise als Nachricht im Short Message Service (SMS), als Nachricht im Multimedia Message Service (MMS), als E-Mail oder als Instant Message, usw. erfolgen.

3.) Der Herunterlad-Klient HK stellt die Informationen für den Benutzer beispielsweise auf einer Anzeige des Mobiltelefons A dar und überprüft, ob der/die in der Beschreibungsinformation BI1 aufgeführten Inhalts-Typen von dem Mobiltelefon A genutzt werden können. Das bedeutet, es wird überprüft, ob das Mobiltelefon A in der Lage ist, bestimmte Inhalte, wie Bilddaten mit einer bestimmten Auflösung oder Farbe oder auch Musikdaten anzeigen oder abspielen zu können. Ist dies der Fall und gibt der Benutzer seine Zustimmung, so fordert der Herunterlad-Klient HK die Übertragung des Bestätigungsobjekts DCFV an, woran in diesem Beispiel logisch an die Anforderung für das eigentliche Rechte-Objekt RO geknüpft ist.

4.) Der Herunterlad-Server überträgt als Antwort auf die Anfrage das Bestätigungsobjekt DCFV an den Herunterlad-Klienten HK.

5.) Der Herunterlad-Klient HK erkennt den Typ des Bestätigungsobjekts DCFV, hat für diesen Objekt- oder Dateityp eine Zuordnung zum DRM-Agenten DRMA gespeichert und übergibt das Bestätigungsobjekt an den DRM-Agenten zur Überprüfung.

6.) Der DRM-Agent überprüft, ob die in dem Bestätigungsobjekt DCFV enthaltene Prüfsumme (oder der Hash-Wert) mit der Prüfsumme (oder dem Hash-Wert) des bereits auf dem Mobiltelefon A gespeicherten Container-Objekt DCF übereinstimmt. Dazu ist in dem Bestätigungsobjekt DCFV auch die Identifikationsbezeichnung des Container-Objekts DCF enthalten. Zu dieser Identifikationsbezeichnung hat der DRM-Agent DRMA die Information gespeichert, wo im Speicher des Mobiltelefons A das entsprechende Container-Objekt abgelegt ist, welchen Wert die Prüfsumme (oder der Hash-Wert) des Container-Objekts oder des in diesem verpackten verschlüsselten Nutzdaten-Objekts hat, und ob die Überprüfung bzw. der Vergleich der Prüfsummen (oder der Hash-Wert) erfolgreich durchgeführt wurde.

7.) Wenn unter 6.) das passende Container-Objekt gefunden wurde und die Prüfsumme (oder der Hash-Wert) erfolgreich überprüft wurde, d.h. wenn die in dem Bestätigungsobjekt enthaltene Prüfsumme mit der Prüfsumme des auf dem Mobiltelefon A gespeicherten Container-Objekts oder dem darin enthaltenen, verschlüsselten Nutzdaten-Objekt übereinstimmt, gibt der DRM-Agent DRMA eine positive Meldung an den Herunterlad-Klienten HK ab.

8.) Der Herunterlad-Klient HK sendet einen Statusbericht an den Herunterlad-Server HS, in dem das unter 7.) erhaltene Ergebnis weitergereicht wird.

9.) Bei Erhalt eines positiven Statusberichts überträgt der Herunterlad-Server die angeforderten Rechte mit dem eigentlichen Rechte-Objekt RO beispielsweise in einem "Push"-Modus (z.B. per WAP-Push) an das Mobiltelefon A. Es ist durchaus möglich, dass eine derartige Übertragung auch mittels einer Nachricht im MMS oder als E-Mail erfolgen kann. Der DRM-Agent DRMA empfängt nun das Rechte-Objekt RO und legt es in einem speziellen Speicherbereich

ab, der vor unberechtigtem Zugriff geschützt ist. Mit dem im Rechte-Objekt RO enthaltenen Schlüssel kann der DRM-Agent DRMA das im Container-Objekt DCF enthaltene, verschlüsselte Nutzdaten-Objekt entschlüsseln und schließlich für den Gebrauch durch den Benutzer des Mobiltelefons nutzbar machen. Beispielsweise können im Nutzdaten-Objekt enthaltene Bilddaten auf einer Anzeigeeinrichtung des Mobiltelefons angezeigt werden, können Musikdaten hörbar abgespielt werden oder können auch multimediale Daten wie Videoclips angezeigt und abgespielt werden usw.

Nach dieser Erläuterung eines allgemeinen Beispiels zur Übertragung bzw. zum Herunterladen von Rechten bzw. Rechte-Objekten von einer Datenbereitstellungskomponente auf eine Telekommunikationseinrichtung, wie einem Bildtelefon, soll nun ein konkreteres Beispiel erläutert werden.

Als Ausgangszustand sei angenommen, dass auf dem Mobiltelefon (A) ein Container-Objekt vorliegt, das per Superdistribution (d.h. eine Übertragung von einem weiteren Mobiltelefon) auf das Mobiltelefon (A) gelangt ist. Beispielsweise wurde das Container-Objekt DCF als Bestandteil einer Multimedia-Nachricht im Multimedia Messaging Service (MMS) oder einfach über eine Infrarotschnittstelle (IrDA) auf das Mobiltelefon (A) übertragen. Es ist dann in einem für Datenobjekte bereitgestellten Speicherbereich bzw. in einem Dateisystem des Mobiltelefons (A) abgelegt und ist dort durch eine spezielle Dateiendung als Container-Objekt zu identifizieren. Aktiviert der Benutzer des Mobiltelefons (A) das Container-Objekt (beispielsweise dass er es in einer Dateiverwaltungsanwendung (wie einem Explorer) auswählt, so wird automatisch der DRM-Agent gestartet, der für das angewählte Container-Objekt ein passendes Rechte-Objekt sucht. Es wird davon ausgegangen, dass noch kein Rechte-Objekt für das Container-Objekt auf das Mobiltelefon (A) übertragen worden ist, so dass der DRM-Agent (DRMA) bei seiner Suche nach einem geeigneten Rechte-Objekt nicht fündig wird und dem Benutzer anbietet, Rechte bzw. ein Rechte-

Objekt, aus dem Internet von dem zugehörigen Rechteanbieter zu beschaffen und auf das Mobiltelefon (A) herunterzuladen. Zu diesem Zweck ist in einem Beschreibungsabschnitt im Container-Objekt eine Internet-Adresse oder URL des Rechteanbieters enthalten. Neben der URL des Rechteanbieters ist in dem Beschreibungsabschnitt des Container-Objekts (vgl. dazu auch Figur 3) die Prüfsumme (oder der Hash-Wert) des in dem Container-Objekt verpackten, verschlüsselten Nutzdaten-Objekts gespeichert, mit dem die Integrität bzw. Unversehrtheit des Container-Objekts und somit des verpackten, verschlüsselten Nutzdaten-Objekts überprüft werden kann. Wählt der Benutzer die URL zum Herunterladen neuer Rechte für das verschlüsselte Nutzdaten-Objekt an, wird zum einen die referenzierte URL angewählt und zum anderen vom DRM-Agenten die Prüfsumme (oder der Hash-Wert) für das in dem Container-Objekt verpackte, verschlüsselte Nutzdaten-Objekt ermittelt, um dessen Unversehrtheit zu verifizieren. Das Ergebnis dieser Unversehrtheitsprüfung wird vom DRM-Agenten gespeichert, ebenso wie die Identifikationsbezeichnung für das Container-Objekt und dessen Position im Dateisystem auf dem Mobiltelefon (A).

Das Abrufen der Ressource (Datenbereitstellungskomponente eines Rechteanbieters) unter der im Beschreibungsabschnitt des Container-Objekts angegebenen Adresse ("Rights-Issuer-URL") hat ein Ergebnis, das von der Ausgestaltung durch den Rechte-Anbieter abhängt. Entweder wird eine Web-Seite zurückgegeben (z.B. im HTML (Hypertext Markup Language)-Format oder in einem anderen beispielsweise einem XML-basierten Format), eine Browser-Anwendung wird auf dem Mobiltelefon A gestartet und es folgt eine Browsing-Sitzung, in der der Benutzer des Mobiltelefons (A) eine Adresse zum Starten des Herunterlad-Vorgangs für neue Rechte angeboten wird. Alternativ zur Zurückgabe einer Web-Seite und einer folgenden Browsing-Sitzung kann der Herunterlad-Vorgang direkt durch Abrufen einer Beschreibungsinformation für ein bestimmtes Container-Objekt bzw. das darin enthaltene Nutzdaten-Objekt gestartet werden.

In der Beschreibungsinformation, die von dem Herunterlad-Klienten (HK) des Mobiltelefons (A) verarbeitet wird, kann das zu den angeforderten Rechten passende, verschlüsselte Nutzdaten-Objekt genau so beschrieben werden, als sollte das verschlüsselte Nutzdaten-Objekt selbst heruntergeladen werden. Damit erhält der Benutzer des Mobiltelefons (A) beim Herunterladen neuer Rechte dieselben Informationen, wie beim Herunterladen des verschlüsselten Nutzdaten-Objekts und hat damit dieselbe Grundlage für seine Entscheidung, die angebotene Leistung (Rechte) in Anspruch zu nehmen oder nicht. Im Unterschied zum Herunterladevorgang für das verschlüsselte Nutzdaten-Objekt und das zugehörige Rechte-Objekt wird in der Beschreibungsinformation allerdings als Inhalt-Typ ("Content-Type") für den Herunterladevorgang der Typ eines dem Rechte-Objekt zugeordneten Bestätigungsobjekt angegeben. Dadurch wird der Herunterlade-Klient und auch der Benutzer informiert, dass nur das Rechte-Objekt bzw. ein diesem zugeordnetes Bestätigungsobjekt übertragen werden. Das entsprechende verschlüsselte Nutzdaten-Objekt muss also schon auf dem Mobiltelefon (A) gespeichert sein. Außerdem kann der Herunterlade-Klient auf der Basis der anderen Angaben in der Beschreibungsinformation, die das verschlüsselte Nutzdaten-Objekt betreffen, überprüfen, ob das beschriebene, verschlüsselte Nutzdaten-Objekt bzw. dessen Inhalt auf dem Mobiltelefon (A) auch genutzt werden kann, d.h. ob Eigenschaften, wie Größe, Typ und weitere Eigenschaften des unverschlüsselten Nutzdaten-Objekts zu den Geräteeigenschaften des Mobiltelefons (A) "passen".

Werden alle oben genannten Kriterien erfüllt und entscheidet sich der Benutzer, neue Rechte herunterzuladen, setzt der Herunterlad-Klient den Herunterladevorgang fort, indem er das dem Rechte-Objekt zugeordnete Bestätigungsobjekt vom Herunterlade-Server (HS) anfordert. Der Herunterlade-Server antwortet und sendet das Bestätigungsobjekt an den Herunterlad-Klienten, der den Objekt-Typ des Bestätigungsobjekts erkennt und das Bestätigungsobjekt sogleich an den DRM-Agenten weiterreicht. Der DRM-Agent erhält das Bestätigungsobjekt, entnimmt anhand

der darin enthaltenen Identifikationsbezeichnung für das relevante Container-Objekt, welches (Container-)Objekt kontrolliert werden muss und vergleicht die im Bestätigungsobjekt erhaltene Prüfsumme (oder den Hash-Wert) mit dem im Beschreibungsabschnitt des Container-Objekts enthaltenen entsprechenden Wert bzw. mit dem zuvor ermittelten Wert des verschlüsselten Nutzdaten-Objekts in dem Container-Objekt. Bei Übereinstimmung der Prüfsummen (oder Hash-Werte) steht fest, dass das verschlüsselte Nutzdaten-Objekt im Container-Objekt mit dem zuvor ausgewählten Rechte-Objekt nutzbar sein wird. Der DRM-Agent signalisiert dann dem Herunterlad-Klient eine positive Überprüfung des Bestätigungsobjekts. Daraufhin sendet der Herunterlade-Klient an den Herunterlade-Server einen Statusbericht, in dem der entsprechende Statuswert bzw. Statusbericht den Herunterlade-Server veranlasst, das zuvor ausgewählte Rechte-Objekt beispielsweise per WAP-Push an das Mobiltelefon (A) zu versenden und eventuell die damit verbundene Leistung (die Nutzung des Nutzdaten-Objekts in dem Container-Objekt) dem Benutzer in Rechnung zu stellen. Dies kann dadurch geschehen, dass der Herunterlade-Server einem Vergebührungssystem des Mobilfunknetzes, in dem das Mobiltelefon (A) beheimatet ist, eine Anweisung zukommen lässt, dem Benutzer des Mobiltelefons (A) das heruntergeladene Recht bzw. Rechte-Objekt beispielsweise mit der herkömmlichen Telekommunikationsverbindungsabrechnung in Rechnung zu stellen.

Nach dem Eintreffen des Rechte-Objekts auf dem Mobiltelefon (A) wird dieses aufgrund seines Objekt-Typs wiederum unmittelbar an den DRM-Agenten weitergereicht und von diesem verwaltet. Über einen Datensatz zur Verwaltung bzw. eine Identifikationsbezeichnung des Container-Objekts kann dieses im Speicher des Mobiltelefons (A) lokalisiert und geöffnet werden. Anschließend wird der in dem (neuen) Rechte-Objekt enthaltene Schlüssel zur Entschlüsselung des verschlüsselten Nutzdaten-Objekts im Container-Objekt verwendet und das Nutzdaten-Objekt kann genutzt werden.

Es sei nun auf Figur 3 verwiesen, in der ein Container-Objekt DCF gezeigt ist, das beispielsweise in einem in Figur 2 dargestellten Verfahren verwendet werden kann. Das Container-Objekt DCF umfasst einen Inhaltsabschnitt IA, in dem ein verschlüsseltes Nutzdaten-Objekt vNDO gespeichert ist, und einen Beschreibungsabschnitt BA, in dem eine Identifikationsbezeichnung "Content-ID" für das Container-Objekt DCF, eine Rechteanbieter-URL, die zum Anfordern neuer Rechte genutzt werden kann und eine Prüfsumme (oder Hash-Wert) vorgesehen ist, mit der die Integrität bzw. Unversehrtheit des verschlüsselten Nutzdaten-Objekts oder des gesamten Container-Objekts überprüft werden kann.

Es sei nun auf Figur 4 verwiesen, in der ein Rechte-Objekt RO dargestellt ist, das beispielsweise in dem in Figur 2 dargestellten Verfahren verwendet werden kann. In einem allgemeinen Beschreibungsabschnitt ABA enthält das Rechte-Objekt RO neben anderen möglichen Bezeichnungen bzw. Elementen eine Identifikationsbezeichnung "Content-ID", die zur Identifikation des zugehörigen Container-Objekts DCF dient. Ferner enthält das Rechte-Objekt RO einen Rechtebeschreibungsabschnitt RBA, der zum einen einen Schlüssel zum Entschlüsseln des in dem Container-Objekt DCF enthaltenen, verschlüsselten Nutzdaten-Objekts vNDO und weiterhin eine Beschreibung der Rechte zur Nutzung des verschlüsselten Nutzdaten-Objekts vNDO enthält. Die Beschreibung der Rechte umfassen, wie bereits oben erwähnt, die Definition der Rechte, die der Benutzer durch das übermittelte Rechte-Objekt erhält, um das verschlüsselte Nutzdaten-Objekt zu nutzen, beispielsweise dass er lediglich Musikdaten anhören darf, selbst wenn ferner Bild- oder Videoinformationen in dem verschlüsselten Nutzdaten-Objekt enthalten sind. Er kann aber auch die Rechte zur vollständigen Nutzung des verschlüsselten Nutzdaten-Objekts erhalten, usw.

Es sei nun auf Figur 5 verwiesen, in der ein dem in Figur 4 dargestellten Rechte-Objekt RO zugeordnetes Bestätigungsobjekt DCFV gezeigt ist. Wesentliche Elemente des Bestätigungsobjekts

DCFV sind zum einen die Identifikationsbezeichnung "Content-ID" zur Referenzierung des zugehörigen Container-Objekts DCF, wie es beispielsweise bezüglich Figur 2 erläutert worden ist, und zum anderen die Prüfsumme (oder Hash-Wert), die mit dem entsprechenden Wert des Container-Objekts DCF verglichen werden muss, um eine korrekte Zuordnung von einem neu herunterzuladenden Rechte-Objekt RO und einem bereits auf einer Telekommunikationseinrichtung eines Benutzers vorhandenen Container-Objekt DCF zu gewährleisten.

Es sei abschließend bemerkt, dass obwohl in den dargestellten Ausführungsformen eines Verfahrens zum Herunterladen von Rechte-Objekten stets davon ausgegangen worden ist, dass zwar bereits ein Container-Objekt mit einem darin enthaltenen, verschlüsselten Nutzdaten-Objekt auf der Telekommunikationseinrichtung eines Benutzers gespeichert ist, jedoch noch kein zugehöriges Rechte-Objekt zum Nutzen des verschlüsselten Nutzdaten-Objekts. Es ist jedoch auch möglich, dass neben dem Container-Objekt mit dem darin enthaltenen, verschlüsselten Nutzdaten-Objekt auch ein erstes Rechte-Objekt bereits auf der Telekommunikationseinrichtung des Benutzers gespeichert ist, das somit die Nutzung des verschlüsselten Nutzdaten-Objekts mit den in dem ersten Rechte-Objekt beschriebenen Rechten ermöglicht. Erlauben diese Rechte des ersten Rechte-Objekts jedoch eine teilweise Nutzung des verschlüsselten Nutzdaten-Objekts, so ist es auch möglich, dass der Benutzer der Telekommunikationseinrichtung ein zweites Rechte-Objekt herunterladen bzw. auf seine Telekommunikationseinrichtung übertragen möchte, die eine umfangreichere bzw. vollständige Nutzung des verschlüsselten Nutzdaten-Objekts ermöglicht. In einem derartigen Fall kann der Benutzer wie beispielsweise allgemein bezüglich Figur 2 beschrieben, das zweite Rechte-Objekt anfordern und nach Überprüfung durch ein dem zweiten Rechte-Objekt zugeordneten Bestätigungsobjekt das zweite Rechte-Objekt auf seine Telekommunikationseinrichtung herunterladen, um eine umfangreichere Nutzung des verschlüsselten Nutzdaten-Objekts auf seiner Telekommunikationseinrichtung zu ermöglichen ("Rights-Refresh").

Patentansprüche

1. Verfahren zum Handhaben von verschlüsselten Nutzdaten-Objekten (vNDO) mit folgenden Schritten:

Übertragen eines Container-Objekts (DCF) zu einer ersten Telekommunikationseinrichtung (A), wobei das Container-Objekt (DCF) einen Inhaltsabschnitt (IA), in dem ein verschlüsseltes Nutzdaten-Objekt (vNDO) vorgesehen wird, und einen Beschreibungsabschnitt (BA), in dem eine ermittelte Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO) vorgesehen wird, aufweist;

Extrahieren der Prüfsumme aus dem Beschreibungsabschnitt (BA) des Container-Objekts (DCF);

Erneutes Ermitteln der Prüfsumme des in dem Inhaltsabschnitt (IA) des Container-Objekts (DCF) vorgesehenen, verschlüsselten Nutzdaten-Objekts (NDO);

Vergleichen der extrahierten Prüfsumme mit der erneut ermittelten Prüfsumme, um bei einer Übereinstimmung der beiden Prüfsummen auf eine ordnungsgemäße Übertragung des verschlüsselten Nutzdaten-Objekts (vNDO) schließen zu können.

2. Verfahren nach Anspruch 1, bei dem eine Datenbereitstellungskomponente (D) Nutzdaten-Objekte (NDO) bereitstellt, die gemäß folgender Schritte verarbeitet werden:

Verschlüsseln von einem auf der Datenbereitstellungskomponente (D) bereitgestellten Nutzdaten-Objekt (NDO);

Ermitteln einer Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO);

Erzeugen eines Container-Objekts (DCF) mit einem Inhalts-

abschnitt (IA), in dem das verschlüsselte Nutzdaten-Objekt (vNDO) vorgesehen wird, und einem Beschreibungsabschnitt (BA), in dem die ermittelte Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO) vorgesehen wird;

Übertragen des Container-Objekts (DCF) von der Datenbereitstellungskomponente (D) an die erste Telekommunikationseinrichtung (A).

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem das Container-Objekt (DCF) von der Datenbereitstellungskomponente (D) über zumindest eine weitere Datenbereitstellungskomponente oder zumindest eine weitere Telekommunikationseinrichtung an die erste Telekommunikationseinrichtung (A) übertragen wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem von der Datenbereitstellungskomponente (D) für das verschlüsselte Nutzdaten-Objekt (vNDO) ein Rechte-Objekt (RO) erzeugt wird, das eine Zuordnungsinformation (Content-ID) zum Zuordnen des Rechte-Objekts (RO) zu einem Container-Objekt (DCF) mit einem verschlüsselten Nutzdaten-Objekt (vNDO), eine Entschlüsselungsinformation zum Entschlüsseln des verschlüsselten Nutzdaten-Objekts, und eine Rechteinformation zur Beschreibung der Benutzungsrechte des verschlüsselten Nutzdaten-Objekts aufweist.

5. Verfahren nach Anspruch 4, bei dem von der Datenbereitstellungskomponente (D) ein dem Rechte-Objekt (RO) zugeordnetes Bestätigungsobjekt (DCFV) erzeugt wird, das eine Zuordnungsinformation zum Zuordnen des Rechte-Objekts (RO) zu einem verschlüsselten Nutzdaten-Objekt und eine Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO) aufweist.

6. Verfahren nach Anspruch 5, das ferner folgende Schritte umfasst:

Anfordern seitens der ersten Telekommunikationseinrichtung (A), dass das dem Rechte-Objekt (RO) zugeordnete Bestätigungsobjekt (DCFV) an diese übertragen wird;

Übertragen des Bestätigungsobjekts (DCFV) von der Datenbereitstellungskomponente (D) zu der ersten Telekommunikationseinrichtung (A);

Extrahieren der Prüfsumme aus dem Bestätigungsobjekt (DCFV);

Vergleichen der aus dem Bestätigungsobjekt extrahierten Prüfsumme mit der erneut ermittelten Prüfsumme, um bei einer Übereinstimmung der beiden Prüfsummen auf eine Kompatibilität des dem Bestätigungsobjekt zugeordneten Rechte-Objekts und des auf die erste Telekommunikationseinrichtung (A) in dem Container-Objekt (DCF) übertragenen, verschlüsselten Nutzdaten-Objekts schließen zu können.

7. Verfahren nach einem der Ansprüche 4 bis 6, bei dem seitens der ersten Telekommunikationseinrichtung (A) angefordert wird, das von der Datenbereitstellungskomponente (D) erzeugte Rechte-Objekt (RO) an diese zu übertragen.

8. Verfahren nach einem der Ansprüche 4 bis 6, bei dem das Rechte-Objekt (RO) von der Datenbereitstellungskomponente (D) zu der ersten Telekommunikationseinrichtung (A) übertragen wird, insbesondere wenn anhand einer Übereinstimmung der Prüfsummen des dem Rechte-Objekt zugeordneten Bestätigungsobjekts und des auf die erste Telekommunikationseinrichtung in dem Container-Objekt übertragenen, verschlüsselten Nutzdaten-Objekts eine Kompatibilität festgestellt worden ist.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem nach einem erfolgreichen Vergleichen der extrahierten Prüfsumme

mit der erneut ermittelten Prüfsumme folgende Schritte durchgeführt werden:

Anfordern einer Beschreibungsinformation (BI1) bezüglich des Inhalts des verschlüsselten Nutzdaten-Objekts (vNDO) von einer Datenbereitstellungskomponente (D);

Übertragen der angeforderten Beschreibungsinformation (BI1) von der Datenbereitstellungskomponente (D) an die erste Telekommunikationseinrichtung (A);

Überprüfen, ob der Inhalt mit in der Beschreibungsinformation (BI1) angegebenen Eigenschaften von der ersten Telekommunikationseinrichtung (A) nutzbar ist.

10. Verfahren zum Handhaben von verschlüsselten Nutzdaten-Objekten (vNDO) mit folgenden Schritten:

Bereitstellen eines verschlüsselten Nutzdaten-Objekts (vNDO) in einer ersten Telekommunikationseinrichtung (A);

Anfordern einer Beschreibungsinformation (BI1) bezüglich des Inhalts des verschlüsselten Nutzdaten-Objekts (vNDO) von einer Datenbereitstellungskomponente (D);

Übertragen der angeforderten Beschreibungsinformation (BI1) von der Datenbereitstellungskomponente (D) an die erste Telekommunikationseinrichtung (A);

Überprüfen, ob der Inhalt mit in der Beschreibungsinformation (BI1) angegebenen Eigenschaften von der ersten Telekommunikationseinrichtung (A) nutzbar ist;

Anfordern bei erfolgreicher Überprüfung der in der Beschreibungsinformation (BI1) angegebenen Eigenschaften von einem Bestätigungsobjekt (DCFV) von der Datenbereitstellungskomponente (D), das einem dem verschlüsselten Nutzda-

ten-Objekt zugeordneten Rechte-Objekt (RO) zugewiesen ist, um eine Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts (vNDO) zu überprüfen.

11. Verfahren nach Anspruch 10, bei dem das Rechte-Objekt (RO) von der Datenbereitstellungskomponente (D) zu der ersten Telekommunikationseinrichtung (A) bei erfolgreicher Überprüfung der Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts übertragen wird.

12. Verfahren nach Anspruch 10 oder 11, bei dem das verschlüsselte Nutzdaten-Objekt in einem Inhaltsabschnitt (IA) eines Container-Objekts (DCF) vorgesehen ist.

13. Verfahren nach Anspruch 12, bei dem das Container-Objekt (DCF) ferner einen Beschreibungsabschnitt (BA) aufweist, in dem eine Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO) vorgesehen ist.

14. Verfahren nach Anspruch 13, bei dem in dem Beschreibungsabschnitt (BA) des Container-Objekts (DCF) ferner die Adresse der Datenbereitstellungskomponente zum Anfordern der Beschreibungsinformation und/oder des Bestätigungsobjekts vorgesehen ist.

15. Verfahren nach Anspruch 13 oder 14, bei dem das Bestätigungsobjekt eine Prüfsumme des verschlüsselten Nutzdaten-Objekts (vNDO) aufweist, wobei die Überprüfung der Kompatibilität des Rechte-Objekts und des verschlüsselten Nutzdaten-Objekts durch folgende Schritte erfolgt:

Extrahieren der Prüfsumme aus dem Bestätigungsobjekt (DCFV);

Vergleichen der aus dem Bestätigungsobjekt extrahierten Prüfsumme mit der in dem Beschreibungsabschnitt (BA) des Container-Objekts (DCF) vorgesehenen Prüfsumme, um bei ei-

ner Übereinstimmung der beiden Prüfsummen auf eine Kompatibilität des dem Bestätigungsobjekt zugeordneten Rechte-Objekts und des auf die erste Telekommunikationseinrichtung (A) in dem Container-Objekt (DCF) vorgesehenen, verschlüsselten Nutzdaten-Objekts schließen zu können.

16. Verfahren nach einem der Ansprüche 6 bis 15, dem von der ersten Telekommunikationseinrichtung (A) zu der Datenbereitstellungskomponente (D) eine erste Bestätigungsmitteilung gesendet wird, wenn eine Kompatibilität des dem Bestätigungsobjekt zugeordneten Rechte-Objekts und des auf die erste Telekommunikationseinrichtung (A) in dem Container-Objekt (DCF) übertragenen, verschlüsselten Nutzdaten-Objekts (vNDO) festgestellt worden ist und/oder eine zweite Bestätigungsmitteilung gesendet wird, wenn die erste Telekommunikationseinrichtung das Rechte-Objekt von der Datenbereitstellungskomponente empfangen hat.

17. Verfahren nach Anspruch 7, 8 oder 12 bis 16, bei dem dem der ersten Telekommunikationseinrichtung (A) zugeordneten Telekommunikationsteilnehmer eine Vergebührungsinformation bezüglich des übertragenen Rechte-Objekts (RO) übermittelt wird.

18. Verfahren nach einem der Ansprüche 1 bis 9 oder 13 bis 17, bei dem die Prüfsumme ein nach einem Hash-Algorithmus berechneter Hash-Wert ist.

19. Verfahren nach einem der Ansprüche 1 bis 18, bei dem die erste und/oder die zumindest zweite Telekommunikationseinrichtung Teil eines ersten Telekommunikationsnetzes, insbesondere in der Ausführung eines Mobilfunknetzes sind.

20. Verfahren nach einem der Ansprüche 2 bis 19, bei dem die Datenbereitstellungskomponente Teil eines zweiten Telekommunikationsnetzes ist.

21. Verfahren nach einem der Ansprüche 1 bis 20, bei dem die erste und/oder die zweite Telekommunikationseinrichtung ein Funkmodul umfassen, und insbesondere als ein Mobiltelefon, ein Schnurlostelefon, oder ein tragbarer Computer ausgebildet sind.

22. Verfahren nach Anspruch 21, bei dem die Übertragung von Daten von und zu der ersten und/oder zweiten Telekommunikationseinrichtung mittels WAP-Protokollen erfolgt.

23. Verfahren nach einem der Ansprüche 1 bis 21, bei dem die Übertragung von Daten von und zu der ersten und/oder zweiten Telekommunikationseinrichtung mittels Internet-Protokollen, wie dem Hypertext Transfer Protocol, erfolgt.

24. Verfahren nach einem der Ansprüche 1 bis 23, bei dem die Nutzdaten-Objekte Textinformationen, Audioinformationen, Videoinformationen, ausführbare Programme, Softwaremodule oder eine Kombination dieser Informationen enthalten.

25. Telekommunikationsanordnung umfassend ein Datenbereitstellungssystem mit zumindest einer Datenbereitstellungskomponente (D) sowie zumindest eine erste Telekommunikationseinrichtung (A), wobei die Telekommunikationsanordnung dafür ausgelegt ist, ein Verfahren nach einem der Ansprüche 2 bis 24 durchzuführen.

26. Datenbereitstellungskomponente, die dafür ausgelegt ist, ein Verfahren nach einem der Ansprüche 2 bis 24 durchzuführen.

27. Telekommunikationseinrichtung, die dafür ausgelegt ist, ein Verfahren nach einem der Ansprüche 2 bis 24 durchzuführen.

FIG 1

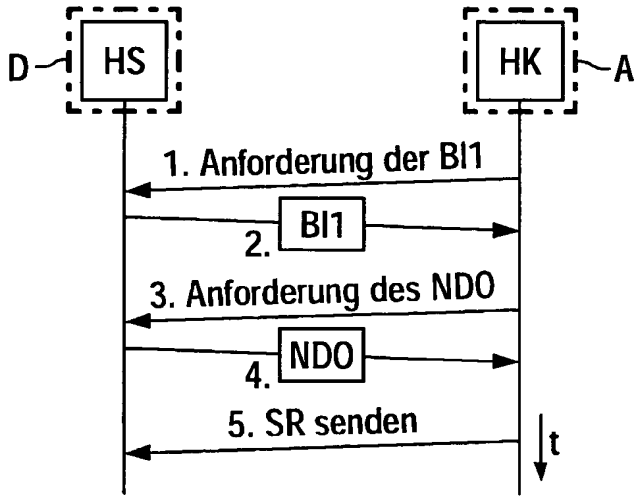

D
HS
HK
A
1. Anforderung der BI1
2.
BI1
3. Anforderung des NDO
4.
NDO
5. SR senden
t

FIG 2

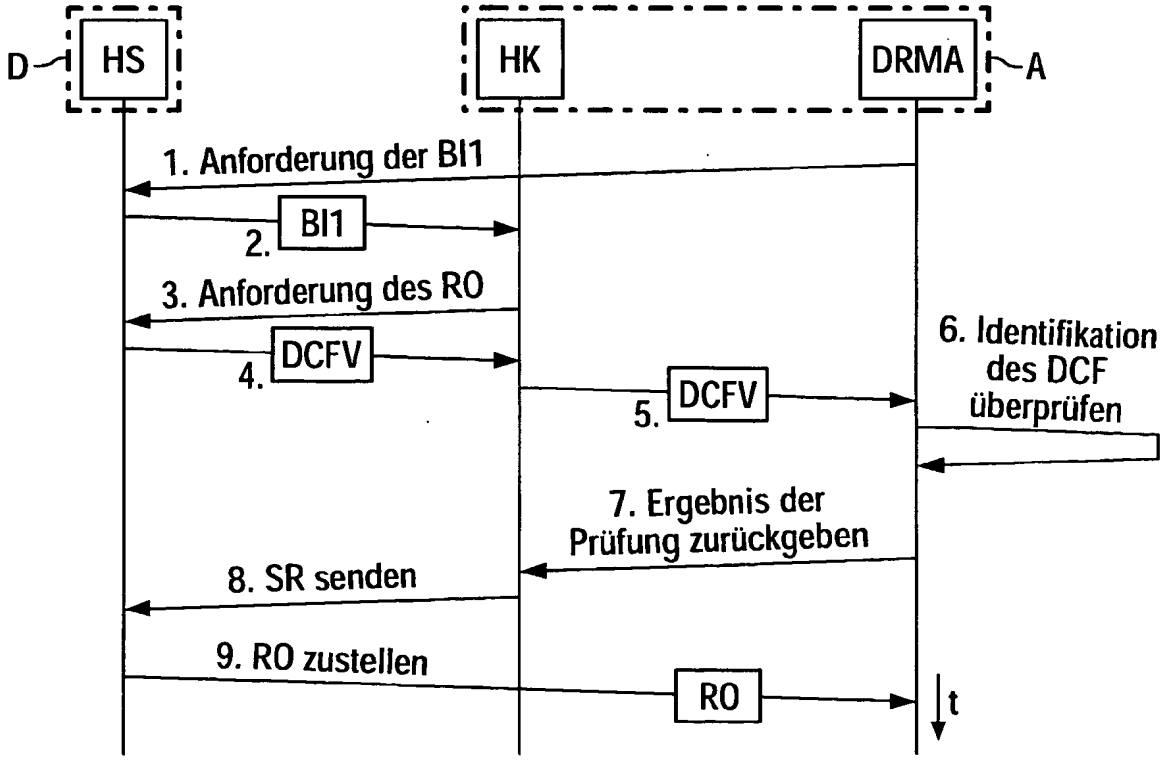

D
HS
HK
DRMA
A
1. Anforderung der BI1
2.
BI1
3. Anforderung des RO
4.
DCFV
5.
DCFV
6. Identifikation des DCF überprüfen
7. Ergebnis der Prüfung zurückgeben
8. SR senden
9. RO zustellen
RO
t

FIG 3

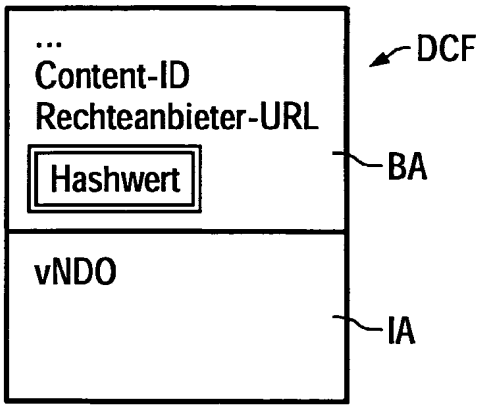


FIG 4

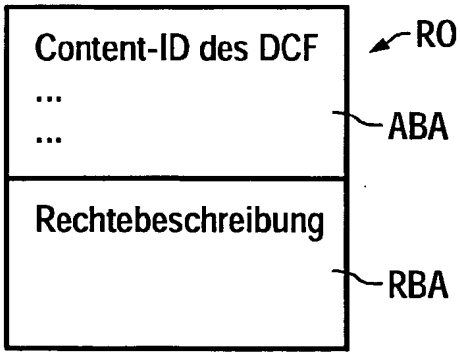


FIG 5